

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-235340

(43)Date of publication of application : 29.08.2000

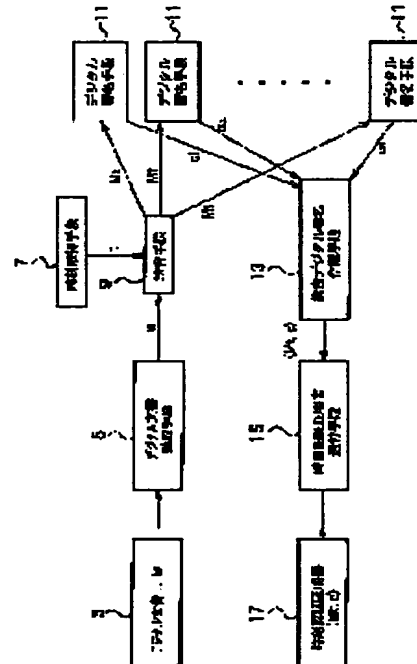
(51)Int.Cl. G09C 1/00
G06F 13/00(21)Application number : 11-035761 (71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>(22)Date of filing : 15.02.1999 (72)Inventor : TAKURA AKIRA
ONO SATOSHI

(54) TIME AUTHENTICATION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a safe and reliable time authentication device for exactly preventing falsification of a time stamp by writing a digital signature with divided plural partial secret keys.

SOLUTION: A digital document (M) 3 prepared by an author is received by a digital document receiving means 5 and coupled to time information (t) from a time acquisition means 7 by a coupling means 9, and a digital document with one time stamp Mt is prepared, and this digital document with time stamp Mt is forwarded to plural digital signature means 11 to prepare digital signatures independently of each other. And, an integrated digital signature preparing means 13 receives the plural digital signatures independently prepared by the plural digital signature preparing means 11 and combines them to prepare an integrated digital signatures (c), and a time authentication certificate forwarding means 15 sends a set of the digital document with time stamp Mt and the integrated digital signature (c) to the author as a time authentication certificate (Mt, c) 17.



LEGAL STATUS

[Date of request for examination] 15.02.1999

[Date of sending the examiner's decision of rejection] 01.07.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3515408

[Date of registration] 23.01.2004

[Number of appeal against examiner's decision of rejection] 2003-14754

[Date of requesting appeal against examiner's decision of rejection] 31.07.2003

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-235340

(P2000-235340A)

(43) 公開日 平成12年8月29日 (2000.8.29)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 8 9
			6 4 0 Z 5 J 1 0 4
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 Z

審査請求 有 請求項の数11 O L (全 20 頁)

(21) 出願番号 特願平11-35761

(22) 出願日 平成11年2月15日 (1999.2.15)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 田倉 昭

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72) 発明者 小野 諭

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100083806

弁理士 三好 秀和 (外1名)

Fターム(参考) 5B089 JA31 JB11 KA17 KC58

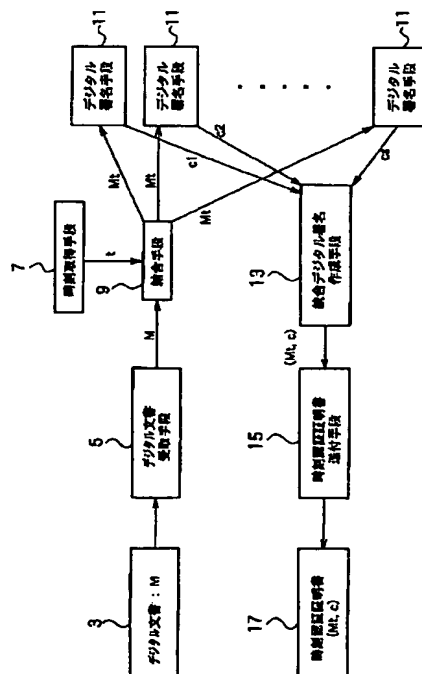
5J104 AA09 AA11 LA03 LA07 PA07

(54) 【発明の名称】 時刻認証装置

(57) 【要約】

【課題】 複数の分割された部分的な秘密鍵でデジタル署名を行うことにより時刻印の偽造を適確に防止し、安全で信頼のおける時刻認証装置を提供する。

【解決手段】 著者が作成したデジタル文書 (M) 3 はデジタル文書受取手段5で受け取られ、結合手段9において時刻取得手段7からの時刻情報tを結合されて、1つの時刻印付デジタル文書Mtが作成され、この時刻印付デジタル文書Mtは複数のデジタル署名手段11に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段11で独立に作成された複数のデジタル署名を統合デジタル署名作成手段13で受け取り結合して、統合デジタル署名cを作成し、時刻認証証明書送付手段15において時刻印付デジタル文書Mtと統合デジタル署名cの組を時刻認証証明書 (Mt, c) 17として著者に送付する。



【特許請求の範囲】

【請求項1】 著者が作成したデジタル文書Mを受け取る文書受取手段と、

時刻情報tを取得する時刻取得手段と、

該時刻取得手段で取得した時刻情報tを前記デジタル文書Mに結合して、1つの時刻印付デジタル文書Mtを作成する結合手段と、

前記時刻印付デジタル文書Mtを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、

該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名cを作成する統合デジタル署名作成手段と、

前記時刻印付デジタル文書Mtおよび統合デジタル署名cの組を時刻認証証明書として著者に送付する時刻認証証明書送付手段とを有することを特徴とする時刻認証装置。

【請求項2】 前記結合手段は、前記時刻印付デジタル文書Mtを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデ

ジタル署名受取手段とを有し、
前記複数のデジタル署名手段の各々は、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Mtを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Mtに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを特徴とする請求項1記載の時刻認証装置。

【請求項3】 著者が作成したデジタル文書Mを受け取り、このデジタル文書Mに認証要求者が必要とする認証の有効期間情報Pを結合するとともにデジタル署名を作成し、更に公開鍵証明書Cを加えた組からなる有効期間付署名要求(MP, Q, C)を送付する有効期間付署名要求手段、および該有効期間付署名要求手段から送付される前記有効期間付署名要求(MP, Q, C)を受け取り、該有効期間付署名要求(MP, Q, C)が正規の契約者からの要求であることを検証し、デジタル文書Mに時刻情報tを結合してデジタル署名した時刻認証証明書(Mt, c)を作成する時刻認証手段を有する時刻認証装置であって、

前記有効期間付署名要求手段は、

著者が作成したデジタル文書Mを受け取るデジタル文書受取手段と、

公開鍵暗号方式における公開鍵と秘密鍵の組を作成し、この作成した公開鍵を前記時刻認証手段に送付する鍵作成手段と、

前記デジタル文書受取手段が受け取ったデジタル文書Mに認証要求者が必要とする認証の有効期間Pを結合して、情報MPを作成する有効期間結合手段と、

前記情報MPに対して秘密鍵を用いてデジタル署名Qを作成するデジタル署名手段と、

前記情報MP、デジタル署名Q、および時刻認証手段から受け取った公開鍵証明書Cの組を有効期間付署名要求(MP, Q, C)として時刻認証手段に送付する有効期間付要求送付手段とを有し、

前記時刻認証手段は、

前記有効期間付署名要求手段から送付される前記公開鍵を受け取り、該有効期間付署名要求手段からの要求

10 に応じて該公開鍵に対するデジタル署名を該時刻認証手段の秘密鍵で作成し、該公開鍵とこの作成されたデジタル署名を組にした公開鍵証明書Cを前記有効期間付署名要求手段に送付する公開鍵証明書返送手段と、

前記有効期間付署名要求手段から送付される有効期間付署名要求(MP, Q, C)を受け取る有効期間付署名要求受取手段と、

この受け取った有効期間付署名要求(MP, Q, C)に含まれるデジタル署名Qおよび公開鍵証明書Cを検証して、署名要求者が正規の契約者であることを確認する有効期間付署名検証手段と、

時刻情報tを取得する時刻取得手段と、

前記有効期間付署名検証手段による検証結果が有効である場合、前記時刻取得手段で取得した時刻情報tが前記有効期間付署名要求(MP, Q, C)に含まれる有効期間Pに含まれるか否かを検証する有効期間内時刻情報検証手段と、

該有効期間内時刻情報検証手段による検証により時刻情報tが有効期間Pに含まれる場合のみ、前記時刻取得手段で取得した時刻情報tを前記有効期間付署名要求(MP, Q, C)に含まれるデジタル文書Mに結合して、時刻印付デジタル文書Mtを作成する時刻情報結合手段と、

前記時刻印付デジタル文書Mtを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名cを作成する統合デジタル署名作成手段と、

前記時刻印付デジタル文書Mtおよび統合デジタル署名cの組を時刻認証証明書(Mt, c)として著者に送付する時刻認証証明書送付手段とを有することを特徴とする時刻認証装置。

【請求項4】 前記時刻情報結合手段は、前記時刻印付デジタル文書Mtを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、

前記複数のデジタル署名手段の各々は、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Mtを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Mtに対して各々独

立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを特徴とする請求項3記載の時刻認証装置。

【請求項5】 前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段および統合デジタル署名作成手段に供給する動作確認手段を更に有し、

前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、

前記統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを特徴とする請求項1記載の時刻認証装置。

【請求項6】 前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給する動作確認手段を更に有し、

前記時刻印付デジタル文書送付手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、

前記デジタル署名受取手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを特徴とする請求項2記載の時刻認証装置。

【請求項7】 公開鍵暗号方式における公開鍵K pと秘密鍵K sの組を作成し、この作成された秘密鍵K sを分割して、前記複数のデジタル署名手段の数の数値の和として表現し、この各数値を1つずつ前記複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、

前記複数のデジタル署名手段の各々は、前記鍵作成・分配手段からそれぞれ配付された秘密鍵を保持し、該秘密鍵を用いた公開鍵暗号方式で前記結合手段から配付された時刻印付デジタル文書M tに対するデジタル署名を作成し、この各デジタル署名手段からの複数のデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名cを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付するように構成されていることを特徴とする請求項1記載の時刻認証装置。

【請求項8】 前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段、統合デジタル署名作成手段、および鍵作成・

分配手段に供給する動作確認手段を更に有し、

前記鍵作成・分配手段は、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に1つずつ配付し、前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、この時刻印付デジタル文書M tを送付された各デジタル署名手段は前記鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書M tに対するデジタル署名を作成し、前記統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名cを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付するように構成されていることを特徴とする請求項7記載の時刻認証装置。

【請求項9】 前記結合手段は、前記時刻印付デジタル文書M tを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有することを特徴とする請求項7記載の時刻認証装置。

【請求項10】 前記デジタル署名手段の各々は、独自に時刻情報t'を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと前記独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成されていることを特徴とする請求項2記載の時刻認証装置。

【請求項11】 公開鍵暗号方式における公開鍵K p2と秘密鍵K s2の組を作成し、この作成された秘密鍵K s2を分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を1つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、

前記時刻認証手段は、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行う動作確認手段を更に有し、

前記デジタル署名手段の各々は、独自に時刻情報t'を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M t

から直ちに時刻情報 t を取得し、この時刻情報 t と前記独自に取得した時刻情報 t' とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成され、

前記鍵作成・分配手段は、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に1つずつ配付し、前記結合手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書 M_t を送付し、デジタル署名手段は、時刻印付デジタル文書 M_t を受信すると、該時刻印付デジタル文書 M_t から直ちに時刻情報 t を取得し、この時刻情報 t と独自に取得した時刻情報 t' とを比較し、両者の差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書 M_t に対するデジタル署名を作成し、統合デジタル署名作成手段は、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を統合デジタル署名作成手段で結合して統合デジタル署名 c を作成し、時刻認証証明書送付手段で時刻印付デジタル文書 M_t 、統合デジタル署名 c 、および公開鍵 K_p2 を組にして時刻認証証明書 (M_t, c, K_p2) として著者に送付するように構成されていることを特徴とする請求項4記載の時刻認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、テキスト文書、画像情報、音声情報等を含むデジタル文書に時刻印を押すことにより時刻印を押された時点以降にデジタル文書が変更されてなく、確かに時刻印が押された時点で対象とするデジタル文書が存在していたことを証明する時刻認証装置に関し、更に詳しくは、インターネット等の不特定多数のユーザが接続されているネットワーク上に時刻認証装置が設置されているときに、時刻認証装置の利用を許可されたユーザ以外の者が不正に時刻認証装置を利用することを防止するとともに、時刻認証証明書が不正に偽造されることを防止し得る時刻認証装置に関する。

【0002】

【従来の技術】この種の時刻認証装置として、従来提案されている例えば特開平7-254897号「個人用日時認証装置」では、スマートカード等に時刻認証装置を組み込み、デジタル署名を行う時に時刻認証と一緒にしている。また、特開平3-185551号「デジタル時間認証装置」では、時刻認証装置を1つのハードウェアプラットフォームとして構成し、文書の作成者がこの装置を使用して時刻認証を行っている。これらの従来の

装置では、いずれも文書作成者が時刻認証を行う方式であるため、偽造し易く、第三者機関による証明でないため、信頼性が乏しい。

【0003】また、特開平6-14018号「電子的公証方法および装置」では、元の文書に対するCRC (Cyclic Redundancy Check)、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行っている。この方式で作成される圧縮文書は、現在広く暗号技術として使用されているMD5やSHA-1などのハッシュ関数を用いて作成される圧縮文書と比較して同一の圧縮文書を持つデジタル文書の偽造がし易い。更に、特開平6-501574号「数値文書に確実にタイムスタンプを押す方法」では、時刻認証を行う外部機関が単独で時刻認証証明書を作成しているが、この方式は外部機関が時刻認証証明書を偽造することが容易である。

【0004】上述した従来の欠点を補うために、従来、受け取った時刻認証要求とその外部機関が直前に発行した時刻認証証明書を結合したデジタル文書に対してハッシュ関数を適用して得られた圧縮文書にデジタル署名を行い、時刻認証証明書を作成する方法を提案しているものがある。この方法は、時刻認証外部機関が時刻認証証明書を偽造することを事実上不可能にしているが、時刻認証証明書が真正であることを証明するには、それ以前に発行した証明書のデジタル署名が必要となる。すなわち、時刻認証外部機関が発行したすべての時刻認証証明書を保存しておかないと、時刻認証証明書が真正であることを証明することができないため、膨大な記憶容量が必要となる。

【0005】

【発明が解決しようとする課題】上述したように、従来の時刻認証装置のうち、特開平7-254897号や特開平3-185551号に提案されている従来の装置では、いずれも文書作成者が時刻認証を行う方式であるため、偽造し易く、第三者機関による証明でないため、信頼性が乏しいという問題がある。

【0006】また、特開平6-14018号のようにCRC、パリティ、検査合計を組み合わせて圧縮文書を作成し、時刻認証を行う従来の方式における圧縮文書は、同一の圧縮文書を持つデジタル文書の偽造がし易いという問題がある。

【0007】更に、特開平6-501574号のように時刻認証を行う外部機関が単独で時刻認証証明書を作成する方式では外部機関が時刻認証証明書を偽造することが容易であるという問題がある。

【0008】上述した従来の欠点を補うために、時刻認証要求と外部機関が直前に発行した時刻認証証明書を結合したデジタル文書にハッシュ関数を適用した圧縮文書にデジタル署名を行い、時刻認証証明書を作成する従来の方法では、時刻認証外部機関が発行したすべての時刻認証証明書を保存しておかないと、時刻認証証明書が真

正であることを証明することができないため、膨大な記憶容量が必要となり、非経済的であるという問題がある。

【0009】また、IETFにおいてハッシュ関数により圧縮されたデジタル文書を外部機関に送付し、この送付されたデジタル文書に対して時刻認証証明書を作成するプロトコルの標準化が進められているが、この方法は外部機関が1ヶ所で時刻認証証明書を作成するため、時刻認証証明書の偽造の可能性および時刻認証証明書を取得することが許されていない悪意のある第三者が不正に時刻認証証明書を取得する危険性を排除することができないという問題がある。

【0010】本発明は、上記に鑑みてなされたもので、その目的とするところは、複数の分割された部分的な秘密鍵でデジタル署名を行うことにより時刻印の偽造を適確に防止し、安全で信頼のおける時刻認証装置を提供することにある。

【0011】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、著者が作成したデジタル文書Mを受け取る文書受取手段と、時刻を取得する時刻取得手段と、該時刻取得手段で取得した時刻情報tを前記デジタル文書Mに結合して、1つの時刻印付デジタル文書Mtを作成する結合手段と、前記時刻印付デジタル文書Mtを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名cを作成する統合デジタル署名作成手段と、前記時刻印付デジタル文書Mtおよび統合デジタル署名cの組を時刻認証証明書として著者に送付する時刻認証証明書送付手段とを有することを要旨とする。

【0012】請求項1記載の本発明にあっては、著者が作成したデジタル文書Mは時刻取得手段からの時刻情報tを結合されて、1つの時刻印付デジタル文書Mtが作成され、この時刻印付デジタル文書Mtは複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるため、複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することなく、記憶容量を大幅に削減し得る。

【0013】また、請求項2記載の本発明は、請求項1記載の発明において、前記結合手段が、前記時刻印付デジタル文書Mtを前記複数のデジタル署名手段に送付す

る時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、前記複数のデジタル署名手段の各々が、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Mtを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Mtに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを要旨とする。

【0014】請求項2記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書Mtを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0015】更に、請求項3記載の本発明は、著者が作成したデジタル文書Mを受け取り、このデジタル文書Mに認証要求者が必要とする認証の有効期間情報Pを結合するとともにデジタル署名を作成し、更に公開鍵証明書Cを加えた組からなる有効期間付署名要求(MP, Q, C)を送付する有効期間付署名要求手段、および該有効期間付署名要求手段から送付される前記有効期間付署名要求(MP, Q, C)を受け取り、該有効期間付署名要求(MP, Q, C)が正規の契約者からの要求であることを検証し、デジタル文書Mに時刻情報tを結合してデジタル署名した時刻認証証明書(Mt, c)を作成する時刻認証手段を有する時刻認証装置であって、前記有効期間付署名要求手段が、著者が作成したデジタル文書Mを受け取るデジタル文書受取手段と、公開鍵暗号方式における公開鍵と秘密鍵の組を作成し、この作成した公開鍵を前記時刻認証手段に送付する鍵作成手段と、前記デジタル文書受取手段が受け取ったデジタル文書Mに認証要求者が必要とする認証の有効期間Pを結合して、情報MPを作成する有効期間結合手段と、前記情報MPに対して秘密鍵を用いてデジタル署名Qを作成するデジタル署名手段と、前記情報MP、デジタル署名Q、および時刻認証手段から受け取った公開鍵証明書Cの組を有効期間付署名要求(MP, Q, C)として時刻認証手段に送付する有効期間付署名要求送付手段とを有し、前記時刻認証手段が、前記有効期間付署名要求手段から送付される前記公開鍵を受け取り、該有効期間付署名要求手段からの要求に応じて該公開鍵に対するデジタル署名を該時刻認証手段の秘密鍵で作成し、該公開鍵とこの作成されたデジタル署名を組にした公開鍵証明書Cを前記有効期間付署名要求手段に送付する公開鍵証明書返

送手段と、前記有効期間付き署名要求手段から送付される有効期間付署名要求（MP、Q、C）を受け取る有効期間付署名要求受取手段と、この受け取った有効期間付署名要求（MP、Q、C）に含まれるデジタル署名Qおよび公開鍵証明書Cを検証して、署名要求者が正規の契約者であることを確認する有効期間付署名検証手段と、時刻情報tを取得する時刻取得手段と、前記有効期間付署名検証手段による検証結果が有効である場合、前記時刻取得手段で取得した時刻情報tが前記有効期間付署名要求（MP、Q、C）に含まれる有効期間Pに含まれるか否かを検証する有効期間内時刻情報検証手段と、該有効期間内時刻情報検証手段による検証により時刻情報tが有効期間Pに含まれる場合のみ、前記時刻取得手段で取得した時刻情報tを前記有効期間付署名要求（MP、Q、C）に含まれるデジタル文書Mに結合して、時刻印付デジタル文書Mtを作成する時刻情報結合手段と、前記時刻印付デジタル文書Mtを受け取って、各々独立にデジタル署名を作成する複数のデジタル署名手段と、該複数のデジタル署名手段で独立に作成された複数のデジタル署名を受け取り結合して、統合デジタル署名cを作成する統合デジタル署名作成手段と、前記時刻印付デジタル文書Mtおよび統合デジタル署名cの組を時刻認証証明書（Mt、c）として著者に送付する時刻認証証明書送付手段とを有することを要旨とする。

【0016】請求項3記載の本発明にあっては、著者が作成したデジタル文書Mを受け取り、このデジタル文書Mに認証要求者が必要とする認証の有効期間情報Pを結合するとともにデジタル署名を作成し、更に公開鍵証明書Cを加えた組からなる有効期間付署名要求（MP、Q、C）を送付し、この送付される有効期間付署名要求（MP、Q、C）を受け取り、この要求が正規の契約者からの要求であることを検証し、検証結果が有効である場合、時刻情報tが有効期間Pに含まれるか否かを検証し、時刻情報tが有効期間Pに含まれる場合のみ、デジタル文書Mに時刻情報tを結合して時刻印付デジタル文書Mtを作成し、この時刻印付デジタル文書Mtを複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるため、複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することなく、記憶容量を大幅に削減し得る。更に、デジタル署名Qと公開鍵証明書Cを検証することにより、署名要求が正規の契約者であることを確認することができる。

【0017】請求項4記載の本発明は、請求項3記載の

発明において、前記時刻情報結合手段が、前記時刻印付デジタル文書Mtを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有し、前記複数のデジタル署名手段の各々が、前記時刻印付デジタル文書送付手段から送付される時刻印付デジタル文書Mtを受け取る時刻印付デジタル文書受取手段と、この受け取った時刻印付デジタル文書Mtに対して各々独立にデジタル署名を作成するデジタル署名作成手段と、この作成されたデジタル署名を前記デジタル署名受取手段に送付する署名送付手段とを有することを要旨とする。

【0018】請求項4記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書Mtを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0019】また、請求項5記載の本発明は、請求項1記載の発明において、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段および統合デジタル署名作成手段に供給する動作確認手段を更に有し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Mtを送付し、前記統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを要旨とする。

【0020】請求項5記載の本発明にあっては、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を結合手段および統合デジタル署名作成手段に供給し、結合手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書Mtを送付し、統合デジタル署名作成手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るため、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【0021】更に、請求項6記載の本発明は、請求項2記載の発明において、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給する動作確認手段を更に有し、前記時

刻印付デジタル文書送付手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、前記デジタル署名受取手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るように構成されていることを要旨とする。

【0022】請求項6記載の本発明にあっては、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を時刻印付デジタル文書送付手段およびデジタル署名受取手段に供給し、時刻印付デジタル文書送付手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、デジタル署名受取手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るため、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【0023】請求項7記載の本発明は、請求項1記載の発明において、公開鍵暗号方式における公開鍵K pと秘密鍵K sの組を作成し、この作成された秘密鍵K sを分割して、前記複数のデジタル署名手段の数の数値の和として表現し、この各数値を1つずつ前記複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、前記複数のデジタル署名手段の各々が、前記鍵作成・分配手段からそれぞれ配付された秘密鍵を保持し、該秘密鍵を用いた公開鍵暗号方式で前記結合手段から配付された時刻印付デジタル文書M tに対するデジタル署名を作成し、この各デジタル署名手段からの複数のデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名cを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付するように構成されていることを要旨とする。

【0024】請求項7記載の本発明にあっては、鍵作成・分配手段は、公開鍵暗号方式における公開鍵K pと秘密鍵K sの組を作成し、この秘密鍵K sを分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を1つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除し、複数のデジタル署名手段の各々は、鍵作成・分配手段から配付された秘密鍵を用いた公開鍵暗号方式で時刻印付デジタル文書M tに対するデジタル署名を作成し、各デジタル署名手段からの複数のデジタル署名を結合して統合デジタル署名cを作成し、時刻印付デジタル文書M t、統合デジタル署名cおよび公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付する。

【0025】また、請求項8記載の本発明は、請求項7記載の発明において、前記複数のデジタル署名手段が正

常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行い、この確認結果を前記結合手段、統合デジタル署名作成手段、および鍵作成・分配手段に供給する動作確認手段を更に有し、前記鍵作成・分配手段が、動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に1つずつ配付し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、この時刻印付デジタル文書M tを送付された各デジタル署名手段は前記鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書M tに対するデジタル署名を作成し、前記統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を前記統合デジタル署名作成手段で結合して統合デジタル署名cを作成し、前記時刻認証証明書送付手段で時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付するように構成されていることを要旨とする。

【0026】請求項8記載の本発明にあっては、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵をデジタル署名手段の数の和に分割し、この分割した秘密鍵を各デジタル署名手段に配付し、結合手段は正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、デジタル署名手段は新たに配付された秘密鍵を用いて時刻印付デジタル文書M tに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、このデジタル署名を結合して統合デジタル署名cを作成し、時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K pを組にして時刻認証証明書(M t, c, K p)として著者に送付するため、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更

に過去に発行した時刻認証証明書は一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができる。

【0027】更に、請求項9記載の本発明は、請求項7記載の発明において、前記結合手段が、前記時刻印付デジタル文書M tを前記複数のデジタル署名手段に送付する時刻印付デジタル文書送付手段と、前記複数のデジタル署名手段から送付される複数のデジタル署名を受け取るデジタル署名受取手段とを有することを要旨とする。

【0028】請求項9記載の本発明にあっては、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、結合手段からの時刻印付デジタル文書M tを時刻印付デジタル文書送付手段から外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るため、外部に設けられた複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0029】請求項10記載の本発明は、請求項2記載の発明において、前記デジタル署名手段の各々が、独自に時刻情報t'を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと前記独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成するように構成されていることを要旨とする。

【0030】請求項10記載の本発明にあっては、各デジタル署名手段は、時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成する。

【0031】また、請求項11記載の本発明は、請求項4記載の発明において、公開鍵暗号方式における公開鍵K p 2と秘密鍵K s 2の組を作成し、この作成された秘密鍵K s 2を分割して、複数のデジタル署名手段の数の数値の和として表現し、この各数値を1つずつ複数のデジタル署名手段の各々に配付し、配付完了後、分割前の秘密鍵を削除する鍵作成・分配手段を更に有し、前記時刻認証手段が、前記複数のデジタル署名手段が正常に動作しているか否を確認するための問い合わせを定期的に各デジタル署名手段に対して行う動作確認手段を更に有し、前記デジタル署名手段の各々が、独自に時刻情報t'を取得する時刻取得手段を更に有し、前記時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと前記独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名

名を作成するように構成され、前記鍵作成・分配手段が、前記動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この新たに作成した秘密鍵を前記複数のデジタル署名手段の数の和に分割し、この分割して得られた秘密鍵を各デジタル署名手段に1つずつ配付し、前記結合手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M tを送付し、デジタル署名手段が、時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて前記結合手段から配付された時刻印付デジタル文書M tに対するデジタル署名を作成し、統合デジタル署名作成手段が、前記動作確認手段からの確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を統合デジタル署名作成手段で結合して統合デジタル署名cを作成し、時刻認証証明書送付手段で時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K p 2を組にして時刻認証証明書(M t, c, K p 2)として著者に送付するように構成されていることを要旨とする。

【0032】請求項11記載の本発明にあっては、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵を複数のデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、結合手段は正常に動作しているデジタル署名手段のみに時刻印付デジタル文書M tを送付し、デジタル署名手段は時刻印付デジタル文書M tを受信すると、該時刻印付デジタル文書M tから直ちに時刻情報tを取得し、この時刻情報tと独自に取得した時刻情報t'とを比較し、差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて時刻印付デジタル文書M tに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を結合して統合デジタル署名cを作成し、時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K p 2を組にして時刻認証証明書(M t, c, K p 2)として著者に送付する。

【0033】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は、本発明の第1の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置において、5は著者が作成

したデジタル文書(M)3を受け取るデジタル文書受取手段、7は時刻を取得する時刻取得手段、9は時刻取得手段7で取得した時刻情報tを前記デジタル文書Mに結合して、1つの時刻印付デジタル文書Mtを作成する結合手段、11は結合手段9から時刻印付デジタル文書Mtを受け取って、各々独立にデジタル署名を作成する複数の、本実施形態ではs個のデジタル署名手段、13は複数のデジタル署名手段11でそれぞれ独立に作成された複数のデジタル署名c1, c2, ..., csを受け取り結合して、統合デジタル署名cを作成する統合デジタル署名作成手段、15は時刻印付デジタル文書Mtおよび統合デジタル署名cの組を時刻認証証明書(Mt, c)17として著者に送付する時刻認証証明書送付手段である。

【0034】このように構成される時刻認証装置において、著者が作成したテキスト文書、音声情報、画像情報またはこれらの組み合わせからなるデジタル文書(M)3は、デジタル文書受取手段5で受け取られ、結合手段9に供給される。結合手段9は、時刻取得手段7を用いて時刻情報tを取得し、この取得した時刻情報tをデジタル文書Mに結合して、時刻印付デジタル文書Mtを作成する。この時刻取得手段7が取得した時刻は、第三者が持つ正確な時計と比較して校正された正確な時計から取得することが望ましい。

【0035】結合手段9で結合された時刻印付デジタル文書Mtは、結合手段9で複数のコピーを作成し、複数のデジタル署名手段11のすべてに送付される。この複数のデジタル署名手段11は、それぞれ受け取った時刻印付デジタル文書Mtに対して保有する秘密鍵を用いてデジタル署名c1, c2, ..., csを作成する。

【0036】このデジタル署名の作成例について説明する。なお、この例では公開鍵暗号の例としてRSAを用いる。RSA公開鍵暗号の説明は、辻井重雄、笠原正雄編著「暗号と情報セキュリティ」(昭晃堂)を参照する。

【0037】pとqを十分大きな素数とし、 $n = pq$ とおく。そして、 $\phi(n) = (p-1)(q-1)$ と互いに素な整数eを適当に定める。すなわち、 $\gcd(e, (p-1)(q-1)) = 1$ とおく。nとeを公開鍵とし、dを $ed = 1 \bmod \phi(n)$ である整数とすると、p, q, dを秘密鍵とする。

【0038】時刻印付デジタル文書MtにMD5やSHA-1等のハッシュ関数を適用して得られるダイジェストをmとする。更に、 $c = m^d \bmod n$ とおく。このとき、組(Mt, c)を統合デジタル署名作成手段13により最終的に作成される統合デジタル署名とする。図1におけるデジタル署名手段11の和をsとする。このとき、dを数の和で表現する。 $d = d_1 + d_2 + \dots + d_s$ とおく。 $c_1 = m^{d_1} \bmod n$, ..., $c_s = m^{d_s} \bmod n$ とす

ると、(Mt, c1), ..., (Mt, cs)がs個のデジタル署名手段11で作成されるデジタル署名となる。本実施形態では、RSA公開鍵暗号を用いたが、楕円公開鍵暗号、DSA(Digital Signature Algorithm)を用いても同様にデジタル署名および統合デジタル署名を作成することが可能である。

【0039】上述したように作成された複数のデジタル署名手段11で作成された複数のデジタル署名c1, c2, ..., csは、各デジタル署名手段11から統合デジタル署名作成手段13に供給され、統合デジタル署名作成手段13で結合され、統合デジタル署名cが作成される。この統合デジタル署名作成手段13で結合作成された統合デジタル署名cは、時刻印付デジタル文書Mtと組にされ、時刻認証証明書送付手段15から時刻認証証明書(Mt, c)17として著者に送付される。

【0040】上述したように、本実施形態では、複数のデジタル署名手段11で各々独自にデジタル署名を行うため、複数のデジタル署名手段11が協同しない限り時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することなく、記憶容量を大幅に削減し得る。

【0041】図2は、本発明の第2の実施形態に係る時刻認証装置の構成を示すブロック図である。

【0042】同図に示す時刻認証装置は、図1に示した第1の実施形態の時刻認証装置における複数のデジタル署名手段11の各々を外部デジタル署名手段19として外部に設け、この外部デジタル署名手段19の各々に時刻印付デジタル文書Mtを送付するMt送付手段21および複数の外部デジタル署名手段19からのデジタル署名を受け取るデジタル署名受取手段23を設けるとともに、また各外部デジタル署名手段19の各々を、Mt送付手段21からの時刻印付デジタル文書Mtを受け取るMt受取手段25、この受け取った時刻印付デジタル文書Mtに対して独立にデジタル署名を作成する前記デジタル署名手段11、およびこの作成されたデジタル署名をデジタル署名受取手段23に送付する署名送付手段27で構成している点が異なるものであり、その他の構成および作用は同じである。

【0043】このように構成される時刻認証装置においては、著者が作成したデジタル文書(M)3は、デジタル文書受取手段5で受け取られ、結合手段9に供給される。結合手段9は、時刻取得手段7を用いて時刻情報tを取得し、この取得した時刻情報tをデジタル文書Mに結合して、時刻印付デジタル文書Mtを作成する。

【0044】結合手段9で結合された時刻印付デジタル文書Mtは、Mt送付手段21に供給され、Mt送付手段21で複数のコピーを作成し、複数の外部デジタル署名手段19のすべてに送付される。

【0045】複数の外部デジタル署名手段19は、それぞれMt送付手段21からの時刻印付デジタル文書MtをMt受取手段25で受け取り、この受け取った時刻印付デジタル文書Mtをデジタル署名手段11に供給する。デジタル署名手段11は、時刻印付デジタル文書Mtに対して保有する秘密鍵を用いてデジタル署名を作成し、署名送付手段27に供給する。署名送付手段27は、デジタル署名手段11で作成されたデジタル署名をデジタル署名受取手段23に送付する。

【0046】デジタル署名受取手段23は、複数の外部デジタル署名手段19の署名送付手段27から送付される複数のデジタル署名c1, c2, ..., csを受け取り、統合デジタル署名作成手段13に供給する。統合デジタル署名作成手段13は、この複数のデジタル署名c1, c2, ..., csを結合して、統合デジタル署名cを作成する。この統合デジタル署名作成手段13で結合作成された統合デジタル署名cは、時刻印付デジタル文書Mtと組にされ、時刻認証証明書送付手段15から時刻認証証明書(Mt, c)17として著者に送付される。

【0047】本実施形態では、複数の外部デジタル署名手段19で各々独自にデジタル署名を行うため、複数の外部デジタル署名手段19が協同しない限り時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0048】図3は、本発明の第3の実施形態に係る時刻認証装置の構成を示すブロック図である。

【0049】同図に示す時刻認証装置は、図1に示した時刻認証装置に対して有効期間付き署名要求を行う機能を設けた点異なるものであり、図1に示した時刻認証装置に相当する機能に有効期間付き署名を検証する有効期間付署名検証手段31および時刻情報tが有効期間Pに含まれるか否かを検証する有効期間内時刻情報検証手段33を付加した時刻認証部35と、著者からデジタル文書(M)3を受け取り、このデジタル文書(M)3に有効期間Pを結合し、更にこの結合されたデジタル文書Mと有効期間Pに対してデジタル署名Qを作成し、このMP, Q, および時刻認証部35から供給される公開鍵証明書Cを組にして有効期間付署名要求(MP, Q, C)として時刻認証部35に送付する有効期間付き署名要求部37とを有する。なお、時刻認証部35は、有効期間付署名検証手段31および有効期間内時刻情報検証手段33に加えて、デジタル文書受取手段5および時刻認証証明書送付手段15しか図示されていないが、実際には、これらに加えて、図1の構成と同じように時刻取得手段7、結合手段9、複数のデジタル署名手段11、および統合デジタル署名作成手段13も有しているものである。

【0050】有効期間付き署名要求部37は、予め公開鍵暗号方式における公開鍵Kpと秘密鍵Ksを作成して保持しており、この作成された公開鍵Kpを時刻認証部

35に送付するようになっている。また、時刻認証部35は、この有効期間付き署名要求部37から送付された公開鍵Kpに対するデジタル署名を時刻認証部35の秘密鍵Ks^{*}で作成し、公開鍵Kpと作成されたデジタル署名を組にした公開鍵証明書Cを有効期間付き署名要求部37に返送するようになっている。

【0051】そして、有効期間付き署名要求部37は、著者からのデジタル文書(M)3を受け取るデジタル文書受取手段39、この受け取ったデジタル文書Mを署名要求者が設定した時刻認証部35が時刻認証を行うことが可能な有効期間Pと結合する結合手段41、この結合されたデジタル文書Mと有効期間PからなるMPに対して秘密鍵Ksを用いてデジタル署名Qを作成するデジタル署名手段43、デジタル文書Mと有効期間Pの結合されたMP、デジタル署名Q、および時刻認証部35から受け取った公開鍵証明書Cを組にして有効期間付署名要求として時刻認証部35に送付する有効期間付署名要求送付手段45から構成されている。

【0052】次に、以上のように構成される時刻認証装置の作用を説明する。著者が作成したデジタル文書

(M)3を有効期間付き署名要求部37のデジタル文書受取手段39で受け取り、結合手段41に送付する。署名要求者は、時刻認証部35が時刻認証を行うことが可能な有効期間Pを設定し、結合手段41は、デジタル文書受取手段39を介して受け取ったデジタル文書Mと有効期間Pを結合し、デジタル署名手段43に送付する。デジタル署名手段43は、MPに対して秘密鍵Ksを用いてデジタル署名Qを作成する。有効期間付署名要求送付手段45は、デジタル文書Mと有効期間Pの結合されたMP、デジタル署名Q、および公開鍵証明書Cを組にして有効期間付署名要求として時刻認証部35に送付する。

【0053】時刻認証部35は、この有効期間付署名要求(MP, Q, C)デジタル文書受取手段5で受け取ると、この有効期間付署名要求(MP, Q, C)に含まれる公開鍵証明書Cが上述したように事前に時刻認証部35が発行した公開鍵証明書Cであるか否かを時刻認証部35の公開鍵Kp^{*}を用いて有効期間付署名検証手段31で検証する。すなわち、時刻認証部35の公開鍵を用いて公開鍵証明書Cを復号し、その結果得られた公開鍵Kpを用いてデジタル署名Qを復号した結果がMPと一致することを検証することにより有効期間付署名要求(MP, Q, C)が時刻認証部35の正規の契約者からの要求であることを確認する。

【0054】デジタル署名Qが、通常公開鍵デジタル署名で行われているように、MPにハッシュ関数を適用した結果に対して、秘密鍵Ksを用いて作成されている場合には、デジタル署名Qを復号して得られる結果がMPにハッシュ関数を適用して結果と一致することを検証する。

10

20

30

40

50

【0055】更に、時刻認証部35は、有効期間内時刻情報検証手段33を用いて、時刻情報tが有効期間Pに含まれることを確認することにより、有効期間付署名要求(MP, Q, C)が今から有効期間P以内に作成されたものであることを検証する。

【0056】また、時刻認証部35は、上述したように、図1に示したと同じ構成を有しているので、有効期間付き署名要求部37から受け取った有効期間付署名要求(MP, Q, C)に含まれるデジタル文書Mを結合手段9に供給し、結合手段9は時刻取得手段7から取得した時刻情報tをデジタル文書Mに結合して、時刻印付デジタル文書Mtを作成する。この時刻印付デジタル文書Mtは、結合手段9で複数のコピーを作成し、複数のデジタル署名手段11のすべてに送付される。この複数のデジタル署名手段11は、それぞれ受け取った時刻印付デジタル文書Mtに対して保有する秘密鍵を用いてデジタル署名c1, c2, ..., csを作成する。

【0057】複数のデジタル署名手段11で作成された複数のデジタル署名c1, c2, ..., csは、各デジタル署名手段11から統合デジタル署名作成手段13に供給され、統合デジタル署名作成手段13で結合され、統合デジタル署名cが作成される。この統合デジタル署名cは、時刻印付デジタル文書Mtと組にされ、時刻認証証明書送付手段15から時刻認証証明書(Mt, c)17として著者に送付される。このように、複数のデジタル署名手段で各々独自にデジタル署名を行うため、時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0058】なお、上記実施形態においては、時刻認証部35は、図1に示した時刻認証装置に対して有効期間付署名検証手段31および有効期間内時刻情報検証手段33を付加した構成のものであると説明したが、図1に示した時刻認証装置の代わりに図2に示したように複数のデジタル署名手段11が外部に設けられ、各々がMt受取手段25、デジタル署名手段11、署名送付手段27からなる複数の外部デジタル署名手段19を有する図2の時刻認証装置を用いてもよいものである。

【0059】図4は、本発明の第4の実施形態に係る時刻認証装置の構成を示すブロック図である。

【0060】同図に示す時刻認証装置は、図3に示した第3の実施形態の時刻認証装置における複数のデジタル署名手段11の各々を外部デジタル署名手段19として外部に設け、この外部デジタル署名手段19の各々に時刻印付デジタル文書Mtを送付するMt送付手段21および複数の外部デジタル署名手段19からのデジタル署名を受け取るデジタル署名受取手段23を時刻認証部35に設けている点が異なるものであり、その他の構成および作用は図3に示した第3の実施形態と同じであるので、その説明は省略する。

【0061】図5は、本発明の第5の実施形態に係る時

刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図1に示した第1の実施形態の時刻認証装置において複数のデジタル署名手段11の動作を確認する動作確認手段49を設けた点が異なるのみであり、その他の構成および作用は図1の時刻認証装置と同じである。

【0062】動作確認手段49は、定期的に複数のデジタル署名手段11の動作を確認するための問い合わせを各デジタル署名手段11に対して行い、一定時間以内に応答があるデジタル署名手段11が正常に動作していると判定し、この判定結果を結合手段9および統合デジタル署名作成手段13に供給するようになっている。また、結合手段9は、動作確認手段49からの判定結果に従って正常に動作しているデジタル署名手段11にのみ時刻印付デジタル文書Mtを送付し、統合デジタル署名作成手段13は、正常に動作しているデジタル署名手段11からのみデジタル署名を受け取るようになっている。

【0063】このように各デジタル署名手段11の動作を確認することにより、デジタル署名手段11が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。正常動作していないと判定されたデジタル署名手段11がある場合には、その判定結果を結合手段9および統合デジタル署名作成手段13に通知する。正常と判定されたデジタル署名手段11は新たな秘密鍵を保持する。結合手段9および統合デジタル署名作成手段13は、正常動作していると判定されたデジタル署名手段11だけからのデジタル署名を用いて統合デジタル署名cを作成する。

【0064】図6は、本発明の第6の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図2に示した第2の実施形態の時刻認証装置に図5に示した動作確認手段49を設けたものであり、具体的には図2に示した第2の実施形態の時刻認証装置において外部に設けた複数の外部デジタル署名手段19の動作を確認する動作確認手段49を設けた点が異なるのみであり、その他の構成および作用は図1の時刻認証装置と同じである。

【0065】動作確認手段49は、定期的に複数の外部デジタル署名手段19の動作を確認するための問い合わせを各外部デジタル署名手段19に対して行い、一定時間以内に応答がある外部デジタル署名手段19が正常に動作していると判定し、この判定結果をMt送付手段21およびデジタル署名受取手段23に供給するようになっている。

【0066】また、Mt送付手段21は、動作確認手段49からの判定結果に従って正常に動作している外部デジタル署名手段19にのみ時刻印付デジタル文書Mtを送付し、デジタル署名受取手段23は、正常に動作しているデジタル署名手段11からのみデジタル署名を受け

取るようになっている。

【0067】このように各外部デジタル署名手段19の動作を確認することにより、図5に示した第5の実施形態の場合と同様に、外部デジタル署名手段19が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。

【0068】図7は、本発明の第7の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図1に示した第1の実施形態の時刻認証装置に対して鍵作成・分配手段51を設けた点が異なるものであり、その他の構成および作用は同じである。

【0069】鍵作成・分配手段51は、公開鍵暗号方式における公開鍵Kpと秘密鍵Ksの組を作成し、この作成された秘密鍵Ksを分割して、デジタル署名手段11の数であるs個($s > 1$)の数値の和として表現し、この各数値を1つずつs個のデジタル署名手段11に配付し、配付完了後、分割前の秘密鍵Ksを削除する機能を有する。

【0070】複数のデジタル署名手段11の各々は、鍵作成・分配手段51からそれぞれ配付された秘密鍵を保持し、前記結合手段9から配付された時刻印付デジタル文書Mtに対して該秘密鍵を用いて公開鍵暗号方式を用いたデジタル署名c1, c2, ..., csを作成する。

【0071】このように作成された複数のデジタル署名c1, c2, ..., csは、各デジタル署名手段11から統合デジタル署名作成手段13に供給され、統合デジタル署名作成手段13で結合され、統合デジタル署名cが作成される。この統合デジタル署名cは、時刻認証証明書送付手段15に供給され、時刻認証証明書送付手段15は、時刻印付デジタル文書Mt、統合デジタル署名c、および公開鍵Kpを組にして、時刻認証証明書(Mt, c, Kp)として著者に送付する。

【0072】図8は、本発明の第8の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図7に示した第7の実施形態の時刻認証装置において図5の実施形態と同様に複数のデジタル署名手段11の動作を確認する動作確認手段49を設けた点が異なるのみであり、その他の構成および作用は図1の時刻認証装置と同じである。

【0073】動作確認手段49は、図5の実施形態で説明したと同様に、定期的に複数のデジタル署名手段11の動作を確認するための問い合わせを各デジタル署名手段11に対して行い、一定時間以内に応答があるデジタル署名手段11が正常に動作していると判定し、この判定結果を結合手段9および統合デジタル署名作成手段13に供給するようになっていることに加えて、動作確認手段49は各デジタル署名手段11の動作確認の結果、正常に動作していないデジタル署名手段11が1つでもあると判定した場合には、この判定結果を結合手段9、統合デジタル署名作成手段13に加えて鍵作成・分配手

段51にも供給するようになっている。

【0074】そして、鍵作成・分配手段51は、動作確認手段49から正常に動作していないデジタル署名手段11が1つでもあるという判定結果を受け取った場合には、新たな公開鍵Kpおよび秘密鍵Ksを作成し、この作成された秘密鍵Ksを正常に動作していることを確認したデジタル署名手段11の数の和に分割する。そして、この分割して得られた秘密鍵を正常と判定されたデジタル署名手段11の各々の1つずつ配付する。配付後、分割前の秘密鍵を削除する。正常と判定された各デジタル署名手段11は、新たに配付された秘密鍵を保持する。

【0075】また、結合手段9は、動作確認手段49から判定結果の通知を受け取ると、鍵作成・分配手段51が上述したようにデジタル署名手段11に配付した後、正常と判定されたデジタル署名手段11にのみ時刻印付デジタル文書Mtを送付する。

【0076】また、結合手段9は、動作確認手段49からの判定結果に従って正常に動作しているデジタル署名手段11にのみ時刻印付デジタル文書Mtを送付し、統合デジタル署名作成手段13は、正常に動作しているデジタル署名手段11からのみデジタル署名を受け取るようになっている。デジタル署名手段11は、新たに配付された秘密鍵を用いて時刻印付デジタル文書Mtに対してデジタル署名を作成する。統合デジタル署名作成手段13も同様に、正常と判定されたデジタル署名手段11からのみデジタル署名を受け取り、この受け取ったデジタル署名のみを使用して統合デジタル署名cを作成する。この統合デジタル署名cは、時刻認証証明書送付手段15に供給され、時刻認証証明書送付手段15は、時刻印付デジタル文書Mt、統合デジタル署名c、および公開鍵Kpを組にして、時刻認証証明書(Mt, c, Kp)として著者に送付する。

【0077】このように各デジタル署名手段11の動作を確認することにより、デジタル署名手段11が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができる。また、動作確認手段49により各デジタル署名手段11の動作確認を行い、正常に動作していないデジタル署名手段11がある場合には、新たな公開鍵Kpおよび秘密鍵Ksを作成し、この作成された秘密鍵Ksを正常に動作しているデジタル署名手段11の数の和に分割し、この分割により得られた秘密鍵を正常と判定されたデジタル署名手段11の各々に1つずつ配付し、正常と判定されたデジタル署名手段11からのみ時刻印付デジタル文書Mtに対するデジタル署名を受け取るようにするとともに、また複数のデジタル署名手段11が秘密鍵を分割して所有し、それぞれのデジタル署名手段11が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性を少なくするとともに、時刻を取得する手段とデジタル署名を行

う手段を実行するすべての機関が結託しない限り時刻印を偽造することができず、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができる。また、過去に発行した時刻認証証明書を一括保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができる。

【0078】図9は、本発明の第9の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図7に示した第7の実施形態の時刻認証装置において複数のデジタル署名手段11の各々を外部デジタル署名手段19として外部に設け、この外部デジタル署名手段19の各々に時刻印付デジタル文書Mtを送付するMt送付手段21および複数の外部デジタル署名手段19からのデジタル署名を受け取るデジタル署名受取手段23を設けた点が異なるのみであり、その他の構成および作用は図7の実施形態と同じであるので、その説明は省略する。

【0079】図10は、本発明の第10の実施形態に係る時刻認証装置の構成を示すブロック図である。同図に示す時刻認証装置は、図4に示した第4の実施形態の時刻認証装置において、時刻認証部35に動作確認手段49を設けるとともに、鍵作成・分配手段51を設け、更に各外部デジタル署名手段19をMt受取手段25および署名送付手段27に加えて、時刻正当性判定手段55を設けた点が異なるのみであり、その他の構成および作用は図4と同じである。

【0080】各外部デジタル署名手段19に設けられた時刻正当性判定手段55は、各外部デジタル署名手段19がMt送付手段21から受け取った時刻印付デジタル文書Mtに付加されている時刻情報tと各外部デジタル署名手段19で独自に取得した時刻情報t'とを比較し、両者の差が十分小さい場合に限り、各外部デジタル署名手段19において鍵作成・分配手段51で既に作成された秘密鍵を用いて時刻印付デジタル文書Mtに対するデジタル署名を作成し、この作成したデジタル署名を署名送付手段27が時刻認証部35のデジタル署名受取手段23に送付するように構成されているものである。

【0081】更に詳しくは、本実施形態において、有効期間付き署名要求部37の有効期間付署名要求送付手段45からは著者の公開鍵Kpが添付されている有効期間付署名要求(MP, Q, Kp, C)を時刻認証部35に送付するようになっている。Cを時刻認証部35の公開鍵Kp'で復号して得られるKpを用いてQがMPのデジタル署名になっていることを検証する代わりに、(MP, Q, Kp, C)に含まれるKpを用いてQを復号した結果がMPになっていること、およびCを時刻認証部35の公開鍵Kp'で復号してKpが得られることを検証する。デジタル署名Qが、MPにハッシュ関数を適用した結果に対して、秘密鍵Ksを用いて作成されている場合には、デジタル署名Qを復号して得られる結果がM

Pにハッシュ関数を適用して結果と一致することを検証する。

【0082】時刻認証部35に設けられた動作確認手段49は、上述したと同様に、複数の外部デジタル署名手段19が正常に動作しているか否かの動作確認を定期的に行い、正常に動作していない外部デジタル署名手段19が1つでもある場合には、鍵作成・分配手段51に新たな公開鍵Kp2および秘密鍵Ks2の作成を依頼する。鍵作成・分配手段51は、この依頼に応じて新たな公開鍵Kp2および秘密鍵Ks2を作成し、この秘密鍵Ksを正常に動作している外部デジタル署名手段19の数の和に分割し、この分割して得られた秘密鍵を正常に動作している各外部デジタル署名手段19に1つずつ配付する。

【0083】一方、時刻認証部35のデジタル文書受取手段5は、有効期間付き署名要求部37から有効期間付署名要求(MP, Q, Kp, C)を受け取ると、この時に時刻取得手段7から時刻情報tを取得する。それから、図3および図4に示した実施形態と同じ検証を行い、検証の結果、有効と判定された有効期間付署名要求(MP, Q, Kp, C)からデジタル文書Mを取り出し、この取り出したデジタル文書Mに先に取得した時刻情報tを結合手段9で結合する。そして、この結合した時刻印付デジタル文書MtをMt送付手段21から正常に動作している外部デジタル署名手段19に送付する。外部デジタル署名手段19は、この受け取った時刻印付デジタル文書Mtに付加されている時刻情報tと外部デジタル署名手段19が先に取得した時刻情報t'と比較し、両者の差が十分小さい場合に限り、鍵作成・分配手段51で既に作成した秘密鍵を用いて、時刻印付デジタル文書Mtに対するデジタル署名を作成し、この作成したデジタル署名を署名送付手段27から時刻認証部35のデジタル署名受取手段23に送付する。

【0084】デジタル署名受取手段23は、各外部デジタル署名手段19からのデジタル署名を受け取り、統合デジタル署名作成手段13に供給する。統合デジタル署名作成手段13は、各デジタル署名を結合して、統合デジタル署名cを作成する。時刻認証証明書送付手段15は、時刻印付デジタル文書Mt、統合デジタル署名c、および公開鍵Kp2を組にして時刻認証証明書(Mt, c, Kp)として著者に送付する。

【0085】

【発明の効果】以上説明したように、本発明によれば、著者が作成したデジタル文書Mは時刻情報tを結合されて、時刻印付デジタル文書Mtが作成され、この時刻印付デジタル文書Mtは複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証

明書として著者に送付されるので、複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができる。また、過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減し得る。

【0086】また、本発明によれば、複数のデジタル署名手段を外部デジタル署名手段として外部に設け、時刻印付デジタル文書M_tを外部の複数のデジタル署名手段に送付し、この複数のデジタル署名手段の各々で作成された複数のデジタル署名をデジタル署名受取手段で受け取るので、外部に設けられた複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が更に困難であり、安全で信頼のおける時刻認証サービスが可能である。

【0087】更に、本発明によれば、著者が作成したデジタル文書Mを受け取り、このデジタル文書Mに認証要求者が必要とする認証の有効期間情報Pを結合するとともにデジタル署名を作成し、更に公開鍵証明書Cを加えた組からなる有効期間付署名要求(MP, Q, C)を送付し、この送付される有効期間付署名要求(MP, Q, C)を受け取り、この要求が正規の契約者からの要求であることを検証し、検証結果が有効である場合、時刻情報tが有効期間Pに含まれるか否かを検証し、時刻情報tが有効期間Pに含まれる場合のみ、デジタル文書Mに時刻情報tを結合して時刻印付デジタル文書M_tを作成し、この時刻印付デジタル文書M_tを複数のデジタル署名手段に送付され、各々独立にデジタル署名を作成され、この複数のデジタル署名手段で独立に作成された複数のデジタル署名を結合して、統合デジタル署名を作成し、この統合デジタル署名および時刻印付デジタル文書の組を時刻認証証明書として著者に送付されるので、複数のデジタル署名手段による各々独自のデジタル署名により時刻印の偽造が困難であり、安全で信頼のおける時刻認証サービスが可能であるとともに、秘密鍵盗難の危険を低減することができ、また過去に発行した時刻認証証明書を保管することもなく、記憶容量を大幅に削減でき、更にデジタル署名Qと公開鍵証明書Cを検証することにより、署名要求が正規の契約者であることを確認することができる。

【0088】本発明によれば、動作確認手段により各デジタル署名手段の動作を確認し、この確認結果を結合手段および統合デジタル署名作成手段に供給し、結合手段は確認結果に基づき正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M_tを送付し、統合デジタル署名作成手段は確認結果に基づき正常に動作しているデジタル署名手段からのみデジタル署名を受け取るので、デジタル署名手段が悪意のある第三者により例えばメモリダンプ等を用いて秘密鍵の盗難にあっていないことを確認することができる。

【0089】また、本発明によれば、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵をデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、正常に動作しているデジタル署名手段のみに対して時刻印付デジタル文書M_tを送付し、デジタル署名手段は新たに配付された秘密鍵を用いて時刻印付デジタル文書M_tに対するデジタル署名を作成し、正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、このデジタル署名を結合して統合デジタル署名cを作成し、時刻印付デジタル文書M_t、統合デジタル署名c、および公開鍵K_pを組にして時刻認証証明書(M_t, c, K_p)として著者に送付するので、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、時刻認証外部機関が1つの秘密鍵を用いてデジタル署名を行う場合の秘密鍵の盗難の危険性や著者と時刻認証外部機関が結託して過去にさかのぼって時刻印を押す偽造の危険性を排除することができ、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更に過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができ、また更にデジタル署名と公開鍵証明書を検証することにより、署名要求が正規の契約者であることを確認することができ、正規の契約者以外の者が不正に時刻認証サービスを受けることを防止することができる。

【0090】更に、本発明によれば、各デジタル署名手段は時刻印付デジタル文書M_tを受信すると、該時刻印付デジタル文書M_tから直ちに時刻情報tを取得し、この時刻情報tと独自に取得した時刻情報t'とを比較し、両者の差が所定の許容時間差以内であるときのみ、デジタル署名を作成する。

【0091】本発明によれば、鍵作成・分配手段は動作確認手段から正常に動作していないデジタル署名手段があるという動作確認結果を受け取ると、新たな公開鍵および秘密鍵を作成し、この秘密鍵を複数のデジタル署名手段の数の和に分割し、この秘密鍵を各デジタル署名手段に配付し、正常に動作しているデジタル署名手段のみに時刻印付デジタル文書M_tを送付し、デジタル署名手段は時刻印付デジタル文書M_tを受信すると、該時刻印付デジタル文書M_tから直ちに時刻情報tを取得し、この時刻情報tと独自に取得した時刻情報t'とを比較

し、差が所定の許容時間差以内であるときのみ、鍵作成・分配手段から配付された秘密鍵を用いて時刻印付デジタル文書M tに対するデジタル署名を作成し、統合デジタル署名作成手段は正常に動作しているデジタル署名手段からのみデジタル署名を受け取り、この受け取ったデジタル署名を結合して統合デジタル署名cを作成し、時刻印付デジタル文書M t、統合デジタル署名c、および公開鍵K p 2を組にして時刻認証証明書(M t、c、K p 2)として著者に送付するので、各デジタル署名手段の動作確認により、デジタル署名手段が悪意のある第三者によりメモリダンプ等を用いて、秘密鍵の盗難にあっていないことを確認することができ、また正常に動作していないデジタル署名手段がある場合には、新たに作成した分割秘密鍵で各デジタル署名手段が独立にデジタル署名を行うことにより、秘密鍵盗難の危険性が少なくなるとともに、時刻取得手段および各デジタル署名手段がすべて結託しない限り時刻印を偽造することができず、時刻認証外部機関が1つの秘密鍵を用いてデジタル署名を行う場合の秘密鍵の盗難の危険性や著者と時刻認証外部機関が結託して過去にさかのぼって時刻印を押す偽造の危険性を排除することができ、安全で信頼のおける時刻認証サービスを行う時刻認証外部機関を運営することができ、更に過去に発行した時刻認証証明書を一切保管する必要がなく、従来に比較し、大幅に記憶容量を低減することができ、また更にデジタル署名と公開鍵証明書を検証することにより、署名要求が正規の契約者であることを確認することができ、正規の契約者以外の者が不正に時刻認証サービスを受けることを防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図2】本発明の第2の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図3】本発明の第3の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図4】本発明の第4の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図5】本発明の第5の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図6】本発明の第6の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図7】本発明の第7の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図8】本発明の第8の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図9】本発明の第9の実施形態に係る時刻認証装置の構成を示すブロック図である。

【図10】本発明の第10の実施形態に係る時刻認証装置の構成を示すブロック図である。

【符号の説明】

5 デジタル文書受取手段

7 時刻取得手段

9 結合手段

11 デジタル署名手段

13 統合デジタル署名作成手段

15 時刻認証証明書送付手段

19 外部デジタル署名手段

21 M t送付手段

23 デジタル署名受取手段

31 有効期間付署名検証手段

33 有効期間内時刻情報検証手段

35 時刻認証部

37 有効期間付き署名要求部

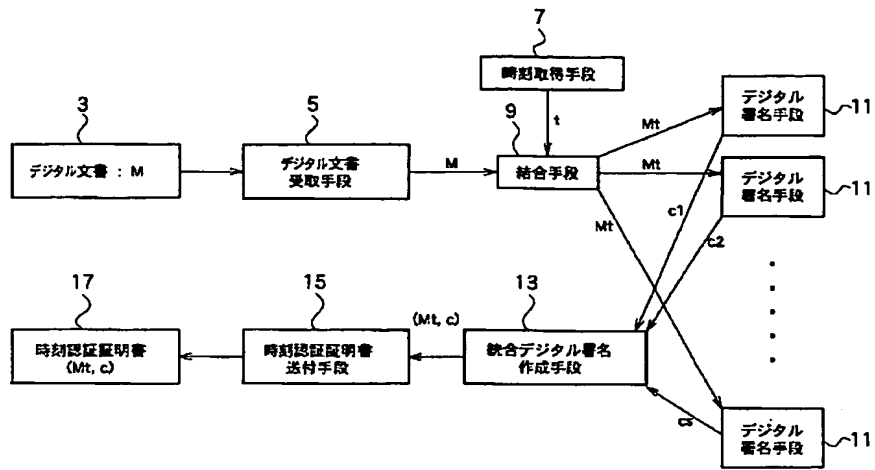
45 有効期間付署名要求送付手段

49 動作確認手段

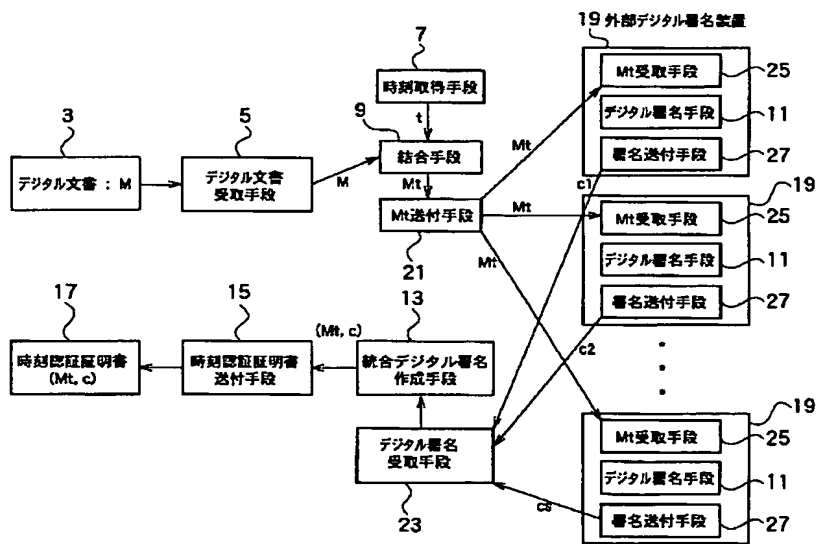
51 鍵作成・分配手段

55 時刻正当性判定手段

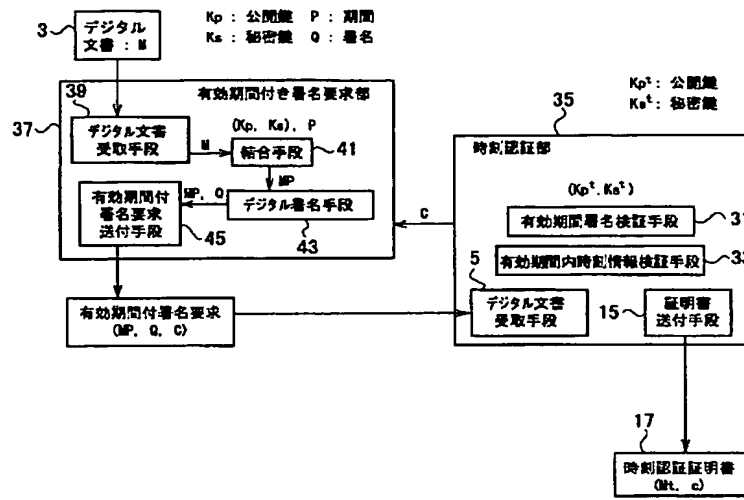
【図1】



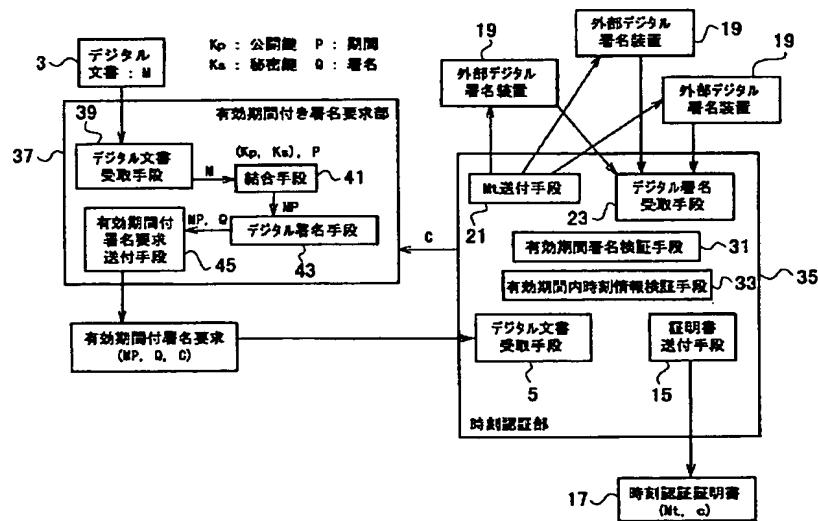
【図2】



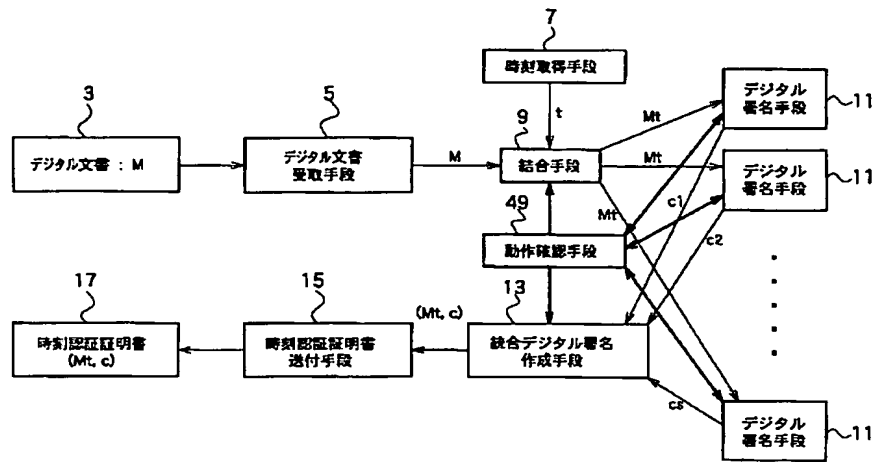
【図3】



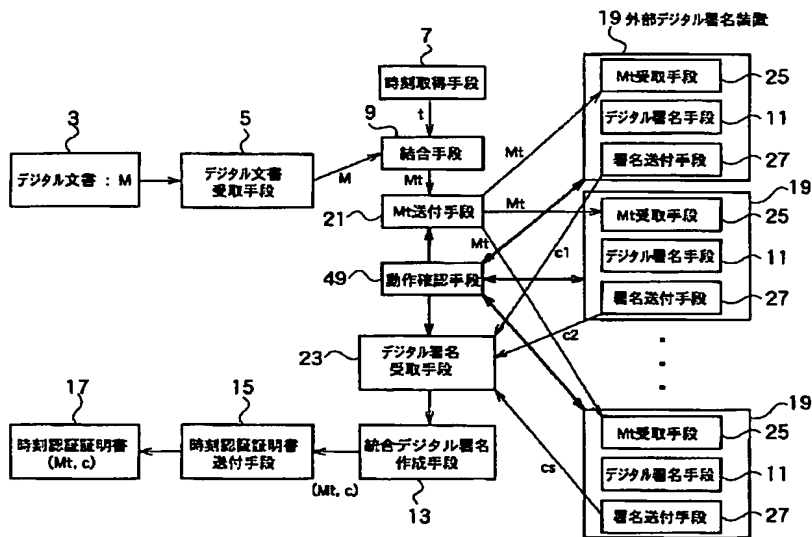
【図4】



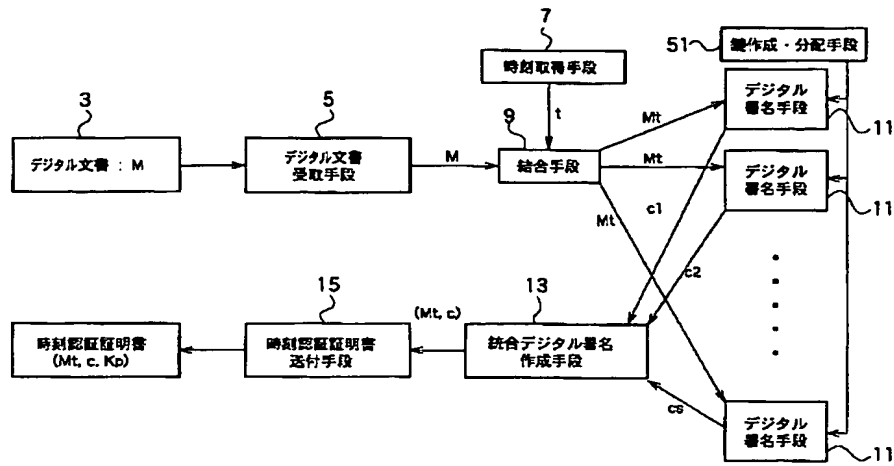
【図5】



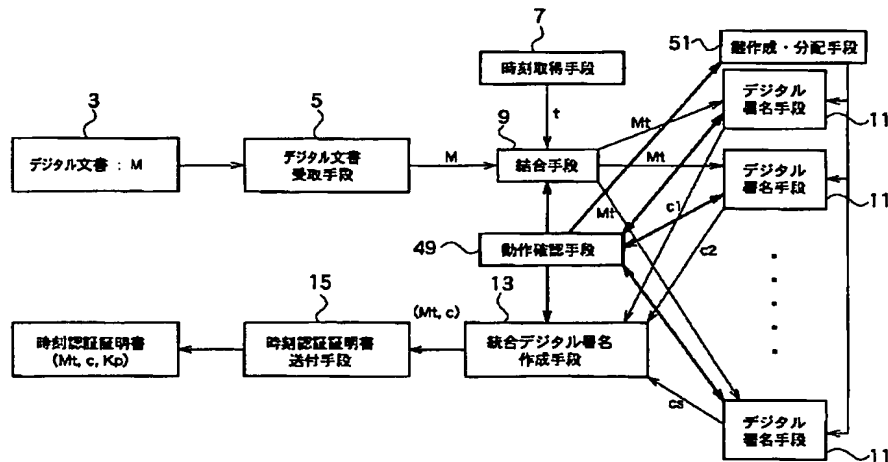
【図6】



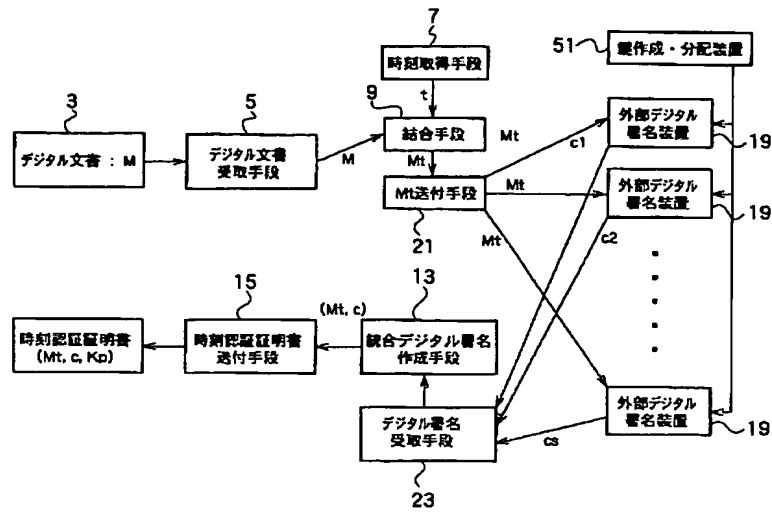
【図7】



【図8】



【図9】



【図10】

